

SEALED

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
FOR A SEARCH WARRANT**

I, Terrance L. Taylor, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been so employed since March 2012. I am currently assigned to the Office of the Resident Agent in Charge HSI Charleston, West Virginia. I have experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks and child pornography possessors and their use of computers and other media devices.

2. Prior to my employment with HSI, I was a Police Officer for two years in Huntington, West Virginia, a Special Agent with the United States Department of State-Bureau of Diplomatic Security for six years, a Special Agent with the Naval Criminal Investigative Service for two years, and a Special Agent with the United States Department of State-Office of Inspector General for two years. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Center ("FLETC") and a graduate of the West Virginia State Police Academy. I graduated from the Criminal Investigator Training Program in 2002, and the Immigration and Customs Enforcement Special Agent Training Program in 2012. As part of

these programs, I received extensive training in the areas of law within the jurisdiction of HSI. I have specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18, United States Code, Sections 2251, 2252, 2252A, and 2256.

3. As a Special Agent, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the FLETC, Immigration and Customs Enforcement, as well as everyday work relating to investigations involving the receipt, possession, access with intent to view, production, importation, advertising, and distribution of child pornography that occur in the Southern District of West Virginia. I have received training in the areas of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have obtained search warrants for child pornography offenses, and I have been the case agent or assisted others in numerous investigations involving the sexual exploitation of children. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), and I am authorized by law to request a search warrant.

4. I make this affidavit in support of an application for a search warrant for information associated with certain Snapchat usernames that are stored at premises owned, maintained, controlled, or operated by Snap Inc. ("Snap"), a social networking company headquartered in Santa Monica, California. The information to be searched is described in the

following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Snap to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B, related to Snapchat accounts for the usernames brock8224, cdaily2002, d_johndob2021, j_jones1778, kohen_t9092, lebronjames8493, michaelj8165, mike_j4407, mjordan6987, and ultimate_w2021 (collectively, the “Subject Accounts”). Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251 (production of child pornography), 2252A (transport, receipt, distribution, possession, and access with intent to view child pornography), 2422(b) (enticement of a minor), and 1519 (destruction of records) (collectively, the “Subject Offenses”) have been committed by TODD CHRISTOPHER ROATSEY (“ROATSEY”). There is also probable cause to search the information described in Attachment A for evidence, contraband, and/or fruits of these crimes further described in Attachment B.

BACKGROUND ON SNAPCHAT¹

7. Snap, Inc. (“Snap”) the owner of Snapchat, is a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Snapchat is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Snapchat accounts like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Snapchat users.

8. Snap collects basic contact and personal identifying information from users during the Snapchat registration process. Snap also collects whether the account phone number has been verified.

9. Snap also collects and retains information about how each user accesses and uses Snapchat. This includes information about the Internet Protocol (“IP”) addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations. Snap also collects account change history, which Snap describes as a log of changes in registration email or phone number, birthdate, and display name.

10. Each Snapchat account is identified by a username.

11. Snapchat offers four primary ways for users to communicate with each other.

¹ The information in this section is based on information published by Snap on its website, including, but not limited to, the following document and webpages: “Snap Inc. Law Enforcement Guide,” available at <https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf>; and “Snapchat Support,” available at <https://support.snapchat.com/>.

a. **Snap.** A user takes a photo or video using their camera phone in real-time. The user then selects a time limit of 1-10 seconds for the receiver to view the photo or video. A user can elect to have the photo/video saved in their phone's photo gallery or just sent via Snapchat, without being saved. The photo/video can then be sent to a friend in Snapchat. The snap is deleted after the selected amount of time. If a recipient attempts to take a screenshot of the snap to save on his/her phone, the application will notify the sender of this behavior. Snapchat states that it deletes each snap from its servers once all recipients have viewed it. If a snap has not been viewed by all recipients, Snapchat states that it retains the snap for thirty days.

b. **Memories.** Memories is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. A user can also edit and send Snaps and create Stories from these Memories. Snaps, Stories, and other photos and videos saved in Memories are backed up by Snapchat and may remain in Memories until deleted by the user.

c. **Stories.** A user can also add the photo/video Snap to their "Story." Depending on the user's privacy settings, the photos and videos added to a Story can be viewed by either all users of Snapchat or just the user's friends for up to 24 hours. Stories can also be saved in Memories.

d. **Chat.** A user can also type messages to friends within the Snapchat app using the Chat feature. A user sends a Chat message to a friend, and once it

is viewed by both parties – and both parties swipe away from the Chat screen – the message will be cleared. Within the Snapchat app itself, a user can opt to save part of the Chat by tapping on the message (text or photo) that he or she wants to keep. The user can clear the message by tapping it again.

12. Snapchat also obtains a variety of non-content information from its users.

13. **Usage Information.** Snapchat may collect information about how users interact with its services, including which search queries they submit, and how they communicate with other users, including maintaining a log of all snaps to and from an account for the last 31 days, for 24 hours of posted Stories, and for any unopened Chats or those saved by a sender or recipient, and how a user interacts with these messages (such as when a user opens a message).

14. **Device Information.** Snapchat collects information about the devices of its users, including information about the user's hardware and software, such as the hardware model, operating system version, device memory, advertising identifiers, unique application identifiers, apps installed, unique device identifiers, browser type, language, battery level, and time zone; information from device sensors, such as accelerometers, gyroscopes, compasses, microphones, and whether the user has headphones connected; and information about the user's wireless and mobile network connections, such as mobile phone number, service provider, and signal strength. Snapchat can also provide the version of the application that is being used, the "last active" date the application was used, and whether two-factor-authentication is enabled.

15. **Device Phonebook.** Snapchat may collect information about the phonebook of the user's device.

16. **Cameras and Photos.** Snapchat may collect images and other information from the user's device.

17. **Location Information.** Snapchat may collect information about the user's location, including precise location using methods that include GPS, wireless networks, cell towers, Wi-Fi access points, and other device sensors, such as gyroscopes, accelerometers, and compasses.

18. **Snap Map.** Snapchat allows a user to share location information with his/her friends and also obtain location information about the user's friends. Based on such information, Snapchat places the friends' locations on a map viewable to the user. Snapchat can provide whether Snap Map was enabled.

19. **Information Collected by Cookies and Other Technologies.** Snapchat may collect information through cookies and other technologies about the user's activity, browser, and device.

20. **Log Information.** Snapchat collects log information when a user uses Snapchat's website, including device information, access times, pages viewed, IP address, and pages visited.

21. In my training and experience, evidence of who was using the above listed usernames and from where, and evidence related to the Subject Offenses, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

22. The stored communications and files connected to a Snapchat account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant

messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. In fact, evidence is included in this affidavit detailing the use of Snapchat by ROATSEY to commit the Subject Offenses.

23. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Snap can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

24. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

25. Therefore, Snap's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Snapchat. In my training and experience,

such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

PROBABLE CAUSE

26. On or about August 22, 2021, MediaLab/Kik submitted CyberTip Report 98779073 to the NCMEC CyberTipline. The CyberTip Report was the result of MediaLab/Kik representatives reporting to NCMEC that a Kik profile bearing the username "jsparrow2174" had uploaded eight (8) videos and one (1) image through Kik Messenger. Kik representatives viewed the aforementioned files and found them to contain depictions of prepubescent and pubescent minors engaged in sexual activity. Kik representatives advised the aforementioned files were sent from "jsparrow2174."

27. On or about September 16, 2021, HSI Charleston issued an administrative subpoena/summons to Suddenlink Communications regarding subscriber information pertaining to the IP address identified in the CyberTip Report. The information provided by Suddenlink indicated that the IP address was assigned to the Elkview, Kanawha County, West Virginia residence owned by Todd Christopher ROATSEY.

28. On October 27, 2021, a federal search warrant was obtained to search the Elkview residence belonging to ROATSEY. The search warrant was executed on October 28, 2021. Law enforcement was present at ROATSEY's residence to execute the search warrant from approximately 6 a.m. to 9 a.m. During the execution of the search warrant, numerous electronic devices were seized. During the execution of the search warrant, numerous electronic devices were seized. Among the items seized was a Samsung tablet consistent with the device that had uploaded the images in the Kik Cybertip. This tablet was found to have been reset to factory settings or

otherwise had its contents removed during the week prior to the execution of the search warrant. However, law enforcement was able to determine from a forensic review of the device that the Kik application had previously been present on the device.

29. Many of the devices seized have been forensically reviewed. The review of one such device, a Samsung Android cell phone seized from ROATSEY at the time of the search, and the microSD card contained therein, (collectively, “the Phone”), revealed evidence of the use of Snapchat.

30. Specifically, review of the Phone revealed multiple screen recordings of Snapchat conversations with minors, some of whom have been identified by law enforcement as students who attended or were attending Pinch Elementary School, where ROATSEY was employed as the school counselor. The recordings were created through the use of screen-recording programs, such as Snapsaver, to make video recordings of all activity that appeared on the cell phone screen during the time when the screen-recording program was active. These recordings were made starting in January 2020 and proceeding through late summer/early fall of 2020. Rather than using his own identity for the Snapchat account in these recordings, ROATSEY pretended to be a teenage boy in order to communicate with multiple minors. The Phone contained saved images of the young male that ROATSEY was using as his fictitious Snapchat persona. ROATSEY’s fictitious profile utilized the display name CDaily and the username cdaily2002. At least two of these minors, neither of whom has yet been identified, sent videos of themselves engaged in sexually explicit conduct at ROATSEY’s direction via Snapchat during January and February 2020. Other minors, some as young as 11 years old, sent videos depicting themselves engaged in sexually suggestive conduct that fell short of the requirements for sexually explicit conduct under federal law.

31. On December 21, 2021, a federal search warrant was obtained for sixteen Google accounts that had been accessed using the Phone. A review of the emails from those Google accounts revealed that defendant had used the email accounts to set up the Subject Accounts.

32. On or about January 5, 2022, a preservation request was sent to Snap regarding the Subject Accounts as well as an administrative subpoena for subscriber information for the Subject Accounts. Eight of the Subject Accounts (brock8224, j_jones1778, kohen_t9092, lebronjames8493, michaelj8165, mike_j4407, mjordan6987, and ultimate_w2021) were identified as still being active Snapchat accounts. The remaining two Subject Accounts (cdaily2002 and d_johndob2021) were reported to have been deleted by the user.

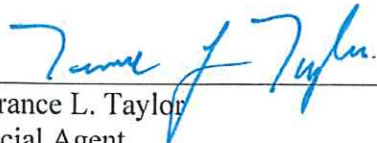
33. Notably, the account for cdaily2002, the account ROATSEY used to pose as a teenage boy in order to receive sexually explicit and sexually suggestive videos of apparent minors, was identified as having been deleted on October 28, 2021, at 1:54 p.m. This was approximately five hours after law enforcement completed its search of ROATSEY's residence; ROATSEY was present during the execution of the search warrant. Due to the account having been deleted, the subscriber information supplied by Snap could only provide the username and deletion date and time for the account. The subscriber information available from the eight active accounts included the associated email address, creation date and time, the creation IP address, and the display name for the account.

CONCLUSION

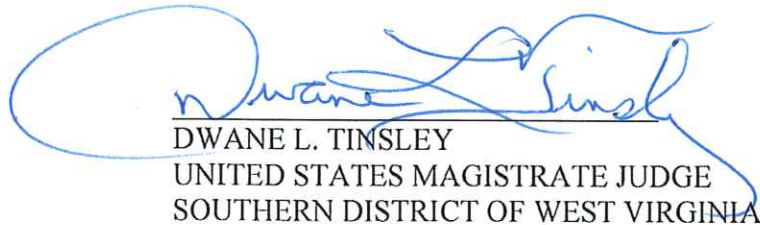
34. Based on the foregoing, there is probable cause to believe that evidence related to the Subject Offenses may be located in the information described in attachment A.

35. Based on the foregoing, I request that the Court issue the proposed search warrant.

36. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Snap. Because the warrant will be served on Snap, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.


Terrance L. Taylor
Special Agent
Department of Homeland Security
Homeland Security Investigations

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this
8th day of February, 2022.


DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA